VIRUSCAN Version 8.3b86
Copyright (C) 1989 - 1992 by McAfee Associates
All rights reserved.
Documentation by Aryeh Goretsky.

McAfee Associates
1900 Wyatt Drive, Suite 8
Santa Clara, CA 95054-1529
U.S.A.

(408) 988-3832 office
(408) 970-9727 fax
(408) 988-4004 BBS 2400 bps
(408) 988-5138 BBS HST 9600
(408) 988-5190 BBS v32 9600
CompuServe GO VIRUSFORUM
InterNet mcafee@netcom.com

TABLE OF CONTENTS:

SYNOPSIS 2
- What VIRUSCAN is, system requirements

AUTHENTICITY 2
- Verifying the integrity of VIRUSCAN

WHAT'S NEW 3
- Features, new viruses added in this release

OVERVIEW 4
- General description of VIRUSCAN

OPERATION. 5
- How to use VIRUSCAN

EXAMPLES 10
- Samples of frequently-used options

EXIT CODES 11
- For running VIRUSCAN from batch files

VIRUS REMOVAL. 11
- How to manually remove a virus

REGISTRATION 11
- How to register VIRUSCAN

TECH SUPPORT 12
- Information you should have ready when calling

APPENDIX A 13
- Creating a virus string file with the /EXT option

APPENDIX B 14
- Miscelleaneous Application Notes

SYNOPSIS

VIRUSCAN (SCAN) is a virus detection and identification program for the IBM PC and compatible computers. VIRUSCAN will search a PC for known computer viruses in memory, the boot sector, the partition table, and the files of a PC and its disks. VIRUSCAN can also detect the presence of unknown viruses.

SCAN works by searching the system for instruction sequences unique to each computer virus, and then reporting their presence when found. This method works for viruses that VIRUSCAN recognizes. SCAN can detect unknown viruses in files and boot sector by appending validation (CRC) codes to .COM and .EXE files and then checking the files against their codes for changes, warning that an infection may have occurred if the file has been modified in any way. An enhanced validation mode is available that will save and check information that can be used by CLEAN-UP to restore infected files, the partition table, or the boot sector of a disk in case of an infection by an unknown virus. SCAN can also check for new viruses from a user-supplied list of virus search strings.

VIRUSCAN runs on any PC with 256Kb and DOS version 2.00 or above.

AUTHENTICITY

VIRUSCAN runs a self-test when executed. If SCAN has been modified in any way, a warning will be displayed. The program will still continue to check for viruses. If SCAN reports that it has been damaged, it is recommended that a clean copy be obtained.

VIRUSCAN versions 46 and above are packaged with the VALIDATE program to ensure the integrity of the SCAN.EXE file. The VALIDATE.DOC instructions tell how to use the VALIDATE program. The VALIDATE program distributed with VIRUSCAN may be used to check all further versions of SCAN.

The validation results for Version 8.3b86 should be:

```
          FILE NAME: SCAN.EXE
               SIZE: 65,936
               DATE: 1-29-1992
FILE AUTHENTICATION
     Check Method 1: 0B8E
     Check Method 2: 0519
```

If your copy of SCAN.EXE differs, it may have been modified. Always obtain your copy of VIRUSCAN from a known source. The latest version of VIRUSCAN and validation data for SCAN.EXE can be obtained off of McAfee Associates' bulletin board system at (408) 988-4004 or from the Computer Virus Help Forum on CompuServe.

Beginning with Version 72, all McAfee Associates programs for download are archived with PKWare's PKZIP Authentic File Verification. If you do not see the "-AV" message after every file is unzipped and receive the message "Authentic Files Verified! # NWN405 Zip Source: McAFEE ASSOCIATES" when you unzip the files then do not run them. If

message may not be displayed. Please contact McAfee Associates if your .ZIP file has been tampered with.

WHAT'S NEW

Version 86-B has been released to fix a false alarm problem with the LZ virus in version 86.

Three new options have been added to this release of VIRUSCAN to allow it to save and check information that can be used by CLEAN-UP to recover infected files, partition tables, or boot sectors infected with unknown viruses. When SCAN is run with the /AG option it will add validation codes to .COM and .EXE files like the /AV option, but will also store information about the file that can be used by CLEAN-UP to reconstruct it if infected by a virus. It will add 52 bytes to COM and EXE files. SCAN will also store copies of the partition table and boot sector in the hidden SCANVAL.VAL file created on the root directory of the bootable harddisk. The /CG option will check this recovery information to determine whether an infection has occurred, and the /RG option will remove this recovery information from the system.

Additionally, a /NOEXPIRE option has been added to prevent display of the SCAN expiration notice when SCAN is more than seven months old.

Of particular interest in this release is the Pogue virus. This virus ' es a new and difficult-to-detect self-mutating engine employing a very sophisticated variable encryption technique loosely based on one developed by the author of Dark Avenger virus and contains code similar to that found in other Bulgarian viruses. The virus was uploaded anonymously to our BBS so it is not clear as to whether it is from Eastern Europe or the USA. It also unknown if the virus is widespread or not.

For a listing of the viruses that were added, please refer to the enclosed VIRLIST.TXT file for a short description. For a more complete description, please refer to Patricia Hoffman's VSUM listing.

THE COMPUSERVE COMPUTER VIRUS HELP FORUM

We are now sponsoring the Computer Virus Help Forum on CompuServe. Updates to VIRUSCAN, information about computer viruses, and technical support may be obtained by typing GO VIRUSFORUM at any CompuServe prompt. A free introductory membership to CompuServe is also available. Please read the COMPUSER.NOT file for details.

OVERVIEW

VIRUSCAN scans diskettes or entire systems for pre-existing computer virus infections. It will identify the virus infecting the system, and tell what area of the system (memory, boot sector, file) the virus occupies. Infected files can be removed with the overwrite-and-delete option, /D, which will erase the file. The CLEAN-UP program is also available to disinfect the system and repair damaged areas of the system whenever possible.

VIRUSCAN Version 86 identifies all known computer viruses along with their variants. Some viruses have been modified so that more than one "strain" exists. Counting such modifications, there are 1,199 virus variants. This includes the twenty most common viruses which account for over 98% of all reported PC infections. The accompanying VIRLIST.TXT file lists describes all viruses identified by SCAN. The number of variants of each virus is listed in parentheses after the virus name.

All known computer viruses infect one or more of the following areas: the hard or fixed disk partition table (also known as the master boot record); the boot sector of hard disks and floppy disks; or one or more executable files within the system. Executable files include operating system files, .COM files, .EXE files, overlay files, or any other files containing program code. A virus that infects more than one area, such as a boot sector and an executable file is called a multipartite virus.

VIRUSCAN identifies every system area or file infected, and indicates both the virus name and CLEAN-UP I.D. code used to remove it. SCAN will check the entire system, an individual diskette, subdirectory, subdirectory tree or individual files for pre-existing virus infection.

VIRUSCAN can also check files for unknown viruses with the Add Validation and Check Validation options. This is done by calculating a checksum for files, appending it to the end of the file, and then comparing the file against it. If the file has been modified, the check will no longer match, indicating that viral infection may have occurred. When run in the enhanced mode, the validation codes will save information that can be used to restore files or areas of the system that have been damaged by an unknown virus.

VIRUSCAN calculates checksums using two independently-generated CRC (Cyclic Redundancy Check). Files which are self-checking or self-modifying should not be validated since this will set off their own internal checks. VIRUSCAN adds validation codes to .COM and .EXE files only. The validation codes for the partition table, boot sector, and system files, are kept in a hidden file called SCANVAL.VAL in the root directory. To detect boot sector and partition table (MBR) viruses, SCAN checks the boot sector and MBR for signs of viral code. If suspicious code is found, SCAN will report it has found a Generic Boot Boot Sector or MBR Virus.

VIRUSCAN can also be updated to search for new viruses via an External Virus Data File option, which allows the user to provide the VIRUSCAN program with new search strings for viruses.

VIRUSCAN can display messages in English, French, or Spanish.

VIRUSCAN works on stand-alone and networked PC's, but not on a file server. For networks, use the NETSCAN file server scanner instead.

An aging notice is built into the SCAN program. When the program is more than seven months old, a notice will be displayed to the user that SCAN may be out of date. SCAN will continue to function normally, however. The aging notice can be bypassed by using the /NOEXPIRE switch.

OPERATION

IMPORTANT NOTE: WRITE PROTECT YOUR FLOPPY DISK BEFORE SCANNING YOUR SYSTEM TO PREVENT INFECTION OF THE VIRUSCAN PROGRAM.

VIRUSCAN will check each area or file on the designated drive(s) that could be host to a virus. If a virus is found, a message is displayed telling the name of the infected file or system area and the name of the identified virus. SCAN will examine files for viruses based on their extensions. The default file extensions supported by SCAN are .APP, .BIN, .COM, .EXE, .OV?, .PGM, .PIF, .PRG, .SWP, .SYS, and .XTP. Additional extensions can be added to SCAN or all files on disk can be selected for scanning.

To run VIRUSCAN type:

```
SCAN d1: ... d26: /? /A /AG filename /AV filename /BELL /CERTIFY /CHKHI /CG
                  /CV /D /DATE /E .xxx .yyy .zzz /EXT filename /FAST
                  /FR /H /HELP /MAINT /MANY /NLZ /NOBREAK / NOEXPIRE /NOMEM
                  /NOPAUSE /NPKL /REPORT filename /RG /RV /SHOWDATE
                  /SP /SUB @filename
```

Options are:

```
              \ - Scan root directory and boot area only
   /? /H /HELP - Display help screen
            /A - Scan all files, including data, for viruses
 /AG filename - Add recovery data/validation codes to specified files
                (the file contains a list of programs
                NOT to add recovery data to)
 /AV filename - Add validation codes to specified files
                (the file contains a list of programs
                NOT to add validation codes to)
       /BELL - Beep whenever a virus is found
    /CERTIFY - List files that do not have a validation code
     /CHKHI - Check memory from 0Kb to 1088Kb
        /CG - Check recovery data/validation codes on files
        /CV - Check validation codes on files
         /D - Overwrite and delete infected file
      /DATE - Save the date and time VIRUSCAN was last run
 /E .xxx .yyy - Scan overlay extensions .xxx .yyy .ZZZ
```

```
          /FAST - Speed up VIRUSCAN's output
            /FR - Display messages in French
             /M - Scan memory for all viruses
                  (see below for specifics)
         /MAINT - Scan MS-DOS 4.0+ boot sector damaged disk
          /MANY - Scan multiple floppies
```



```
           /NLZ - Skip internal scan of LZEXE compressed files
      /NOBREAK - Disable Ctrl-C / Ctrl-Brk during scanning
     /NOEXPIRE - Do not display expiration notice
       /NOMEM - Skip memory checking
      /NOPAUSE - Disable screen pause when scanning
       /NPKL - Skip internal scan of PKLITE compressed files
/REPORT filename - Create report of infected files
           /RG - Remove recovery data/validation codes from files
           /RV - Remove validation codes from specified files
     /SHOWDATE - Display date and time VIRUSCAN was last run
           /SP - Display messages in Spanish
          /SUB - Scan subdirectories
    @filename - Scan using options from configuration file
  (d1: ... d26: indicate drives to be scanned)
```

The /A option will cause SCAN to check all files on the referenced drive. This should only be used if a file-infecting virus has already been detected. Otherwise the /A option should only be used when checking a new program. The /A option will add a substantial time to scanning. This option takes priority over the /E option.

The /AG option allows the user to store recovery data and validation codes for .COM and, .EXE, files the boot sector, and partition table of a disk. Recovery information adds fifty-two (52) bytes to files. The recovery information for the partition table and boot sector is stored seperately in a hidden file in the root directory. It is otherwise similar to the /AV option below. Recovery requires the CLEAN-UP (CLEAN.EXE) program.

The /AV option allows the user to add validation codes to the files being scanned. If a full drive is specified, SCAN will create validation data for the partition table, boot sector, and system files of the disk as well. Validation adds ten (10) bytes to files; the validation data for the partition table, boot sector, and system files is stored separately in a hidden file in the root directory of the scanned drive. Files which are already immunized against computer viruses or contain self-modifying code should not have validation codes added to them. To prevent VIRUSCAN from adding validation codes to these files, a validation exception list will have to be created with the complete path and filename of the each file NOT to be validated listed on each line. Only one file should be on a line. To put a comment in, start a line with the asterisk "*" character. This sample file contains a list of programs not to validate:

```
*This is MS-DOS 5.00's self-modifying program, SETVER
  \DOS\SETVER.EXE
*PKWare's data compression programs already perform a self-check
C:\PKWARE\PKLITE.EXE
C:\PKWARE\PKZIP.EXE
C:\PKWARE\PKUNZIP.EXE
*Stac Technologies hard disk swapping program
C:\SWAPVOL.COM
*Symantec's Norton Utilities V6.01 disk caching program
```

*WordStar
C:\WORDSTAR\WS.EXE

The validation exception list should be an ASCII text file. If a word processor is used to create the list, be sure to save the file as ASCII.

The /BELL option will cause VIRUSCAN to beep each time a computer virus is found.

The /CERTIFY option will audit a system for files that have validation codes added to them with the /AV switch. Files that have no validation code will be reported as being uncertified by VIRUSCAN.

The /CHKHI option checks the memory above 640Kb that can be used on AT (286) and 386 systems for computer viruses. This includes the 384Kb Upper Memory Area from 640Kb to 1024Kb, and the 64Kb High Memory Area from 1024Kb to 1088Kb. On XT systems with extended memory cards installed, this will cause the first 64K of RAM to be scanned again. This option can not be used with the /NOMEM option.

The /CG option checks restoration information and validation codes inserted by the /AG option. If the file or system area has been changed, SCAN will report that the file has been modified.

The /CV option checks validation codes inserted by the /AV option. If the file has been changed, SCAN will report that the file has been modified, and that viral infection may have occurred. Using the /CV option adds about 25% more time to scanning.

NOTE: Some older Hewlett Packard and Zenith PC's modify the boot sector or partition table each time the system is booted. This will cause SCAN to continually notify the user of boot sector or partition table modifications if the /CV switch is selected. Check your system's manual to determine if your system contains self-modifying boot code.

The /D option tells VIRUSCAN to prompt the user to overwrite and delete an infected file when one is found. A file erased by the /D option can not be recovered. If the McAfee Associates' CLEAN-UP program is available, it can be used to disinfect the file. Boot sector and partition table infectors can not be removed by the /D option and require the CLEAN-UP virus disinfection program.

The /FAST option will speed VIRUSCAN up by displaying less information on the screen during scanning, skipping scanning inside of LZEXE- and PKLITE-compressed files, and examining a smaller portion of files during scanning. This may reduce the accuracy of SCAN.

The /E option allows the user to specify an extension or set of extensions to scan. Extensions should include the period character "." and be separated by a space after the /E and between each other. Up to three extensions may be added with the /E. For more extensions, use the /A option.

The /EXT option allows VIRUSCAN to search for viruses from a text file containing user-defined search strings in addition to the viruses that already SCAN checks for. The syntax for using the external virus data file is /EXT d:filename, where d: is the drive letter and filename is the name of the external virus data file. For instructions on how to create an external virus data file, refer to Appendix A.

NOTE: The /EXT option is intended for users to add strings for detection of computer viruses on an interim or emergency basis. When used with the /D option, it will delete infected files. This option is not recommended for general use and should be used with caution.

The /FR option tells VIRUSCAN to output all messages in French instead of English.

The /M option tells VIRUSCAN to check system memory for all known computer viruses that can inhabit memory. SCAN by default only checks memory for critical and "stealth" viruses, which are viruses which can cause catastrophic damage or spread the infection during the scanning process. SCAN will check memory for the following viruses in any case:

1024	1253	1554	1963
1971	2560	337	3445-Stealth
4096	512	Anthrax	Antitelefonica
Brain	Caz	CD	Dark Avenger
DIR-2	Doom II	Empire	Fish
Flu-2	Form	Greemlin	Irish
Joshi	Leech	Lozinsky	Microbes
Mirror	Nomenklatura	NOP	No-Int (Stoned III)
P1R (Phoenix)	Phantom	Plastique	Pogue
SBC	Sentinel	Stoned	Sunday-2
SVC	Taiwan3	Tequila	Turbo (Polish-2)
Twin-351	V2100	V2P6	Whale

If one of these viruses is found in memory, SCAN will stop and advise the user to power down, and reboot the system from a virus-free system disk. Using the /M option with another anti-viral software package may result in false alarms if the other package does not remove its virus search strings from memory. The /M option will add 6 to 20 seconds to the scanning time.

The /MAINT option is used to scan hard disks partitioned with DOS 4.0 or above that have been damaged by a boot sector or partition table infecting virus. Attempts to access disks damaged in such a manner result in an "invalid media" message being displayed. The /MAINT option will only scan the partition table and boot sector, not the files.

The /MANY option is used to scan multiple diskettes placed in a given drive. If the user has more than one floppy disk to check for viruses, the /MANY option will allows the user to check them without having to run SCAN multiple times. If a system has been disinfected, the /MANY and /NOMEM options can be used to speed scanning of disks.

The /NLZ option tells VIRUSCAN not to look inside files compressed with the LZEXE file compression program. SCAN will still check the programs for external infections.

The /NOBREAK option disables Control-C or Control-Break from stopping VIRUSCAN while running.

The /NOMEM option is used to turn off all memory checking for viruses. It should only be used when a system is known to be free of viruses. The /NOMEM option can not be used with the /CHKHI or /M options.

The /NOEXPIRE option disables the aging message that is displayed when SCAN is more than seven months old.

The /NOPAUSE option disables the "More..." prompt that appears when SCAN fills up a screen with data. This allows VIRUSCAN to run on a machine with multiple infections without requiring operator intervention when the screen fills up with messages from the SCAN program.

The /NPKL option tells VIRUSCAN not to look inside files compressed with the PKLITE file compression program. SCAN will still check the programs for external infections.

The /REPORT option is used to generate a listing of infected files. The resulting list is saved to disk as an ASCII text file. To use the report option, specify /REPORT on the command line, followed by the device and filename [See EXAMPLES below for samples].

The /RG option will remove validation codes and recovery information from files added with the /AG option.

The /RV option is used to remove validation codes from a file or files. It can be used to remove the validation code from a diskette, subdirectory, or file(s). Using /RV on a disk will remove the partition table, boot sector, and system file validation. This option can not be used with the /AV option.

The /SP option tells VIRUSCAN to output all messages in Spanish instead of English.

The /SUB option allows SCAN to scan subdirectories under a a subdirectory when scanned. Previously, SCAN would only recursively check subdirectories if a logical device (e.g., C:) was scanned.

The @filename option allows the user to store a list of preferred options and/or areas of the system to be scanned in a configuration file and then have SCAN read the options in and execute them. Options need to be separated by a space, while system areas (a disk or subdirectory or file) need to be on a separate line for each entry. A sample file might look like this:

```
/A /BELL /CV /NOMEM /REPORT C:\VIRUSCAN\SCAN.LOG
C:
D:\BBS
E:\MCAFEE\CLEAN-UP\CLEAN.EXE
```

The first line contains the VIRUSCAN options while the other lines contain the name of files, subdirectories, or disks to be scanned The configuration file should be an ASCII text file. If a word processor is used to create the list, be sure to save the file as ASCII.

EXAMPLES

The following examples are shown as they would be typed in.

SCAN C:
To scan drive C:

SCAN A:R-HOOPER.EXE
To scan file "R-HOOPER.EXE" on drive A:

SCAN A: /A /CV
To scan all files and check validation codes for unknown viruses on drive A:.

SCAN B: /D /A
To scan all files on drive B:, and prompt for erasure of infected files.

SCAN C: D: E: /AV /NOMEM
To add validation codes to files on drives C:, D:, and E:, and skip memory checking.

SCAN C: D: /M /A /FR
To scan memory for all known and extinct viruses, as well as all files on drives C: and D:, and output all messages in French.

SCAN C: D: /E .WPM .COD
To scan drives C: and D:, and include files with the extensions .WPM and .COD

SCAN C: /EXT A:SAMPLE.ASC /BELL
To scan drive C: for known computer viruses and also for viruses added by the user via the external virus data file option, and beep whenever a virus is found.

SCAN C: /M /NOPAUSE /REPORT A:INFECTN.RPT
To scan for all viruses in memory and drive C: without stopping, and create a log on drive A: called INFECTN.RPT

SCAN C: D: /NOPAUSE /REPORT B:VIRUS.RPT
To scan drives C: and D: for viruses without stopping, and create a log on drive B: called VIRUS.RPT

SCAN E:\DOWNLOADS /SUB
To scan all subdirectories under DOWNLOADS on drive E:

SCAN C: D: E: /FAST /CERTIFY
To perform a fast scan of drives C:, D:, and E: and check for any files that do not have validation codes.

SCAN @C:\SCANOPTN.LST
To run VIRUSCAN using configuration file SCANOPTN.LST

EXIT CODES

VIRUSCAN will set the DOS ERRORLEVEL upon program termination to:

ERRORLEVEL	DESCRIPTION
0	No viruses found
1	One or more viruses found
2	Abnormal termination (program error)

If a user stops the scanning process, SCAN will set the ERRORLEVEL to 0 or 1 depending on whether or not a virus was discovered prior to termination of the SCAN. The /NOBREAK option can be used to prevent scanning from being stopped.

VIRUS REMOVAL

What do you do if a virus is found? You can contact McAfee Associates for help with removing viruses by BBS, FAX, telephone, Internet, or CompuServe. There is no charge for support calls to McAfee Associates.

The CLEAN-UP universal virus disinfection program is available and will disinfect the majority of reported computer viruses. It is updated with each release of the SCAN program to remove new viruses. The CLEAN-UP program can be downloaded from McAfee Associates BBS, the SIMTEL20 archives on the InterNet, the McAfee Associates' sponsored Computer Virus Help Forum on CompuServe, or from the agents listed in the enclosed text file.

It is strongly recommended that you get experienced help in dealing with viruses, especially critical viruses that can damage or destroy data [for a listing of critical viruses, see the /M option under OPTIONS, above] and partition table or boot sector infecting viruses, as improper removal of these viruses could result in the loss of all data and use of the disk(s).

For qualified assistance in removing a virus, please contact McAfee Associates directly or check the enclosed AGENTS.TXT file for an Authorized McAfee Associates Agent in your area. Agents may charge McAfee Associates normal support rates for their services.

REGISTRATION

A registration fee of $25.00US is required for the use of VIRUSCAN by individual home users. Registration is for one year [ ] entitles the holder to unlimited free upgrades off of McAfee Associates BBS or CompuServe Computer Virus Help Forum. When registering, a diskette containing the latest version may be requested. Add $9.00US for diskette mailings. Only one diskette mailing will be made.

Registration is for home users only and does not apply to businesses, corporations, organizations, government agencies, or schools who must obtain a license for use. Contact McAfe

Outside of the United States, registration and support may be obtained from the Agents listed in the accompanying AGENTS.TXT file.

TECH SUPPORT

For fast and accurate help, please have the following information prepared when you contact McAfee Associates:

- Program name and version number.
- Type and brand of computer, hard disk, plus any peripherals.
- Version of DOS you are running, plus any TSRs or device drivers in use.
- Printouts of your AUTOEXEC.BAT and CONFIG.SYS files.
- The exact problem you are having. Please be as specific as possible. Having a printout of the screen and/or being at your computer will help also.

McAfee Associates can be contacted by CompuServe Forum, BBS, fax, or InterNet 24 hours a day, or call our business office at (408) 988-3832, Monday through Friday, 8:30AM to 6:00PM Pacific Standard Time.

McAfee Associates	(408) 988-3832 office
4423 Cheeney Street	(408) 970-9727 fax
Santa Clara, CA 95054-0253	(408) 988-4004 BBS 2400 bps
U.S.A	(408) 988-5138 BBS HST 9600
	(408) 988-5190 BBS v32 9600
	CompuServe GO VIRUSFORUM
	Internet mcafee@netcom.com

If you are overseas, please refer to the AGENTS.TXT file for a listing of McAfee Associates Agents for support or sales.

APPENDIX A: Creating a Virus String File with the /EXT Option

The External Virus Data file should be created with an editor or a word processor and saved as an ASCII text file. Be sure each line ends with a CR/LF pair.

NOTE: The /EXT option is intended for emergency and research use only. It is an temporary method for identifying new viruses prior to the subsequent release of SCAN. A sound understanding of viruses and string-search techniques is advised as a prerequisite for using this option.

The virus string file uses the following format:

```
#Comment about Virus_1
"aabbccddeeff..." Virus_1_Name
#Comment about Virus_2
"gghhiijjkkll..." Virus_2_Name
      .
      .
"uvvwwxxyyzz..." Virus_n_Name
```

Where aa, bb, cc, etc. are the hexadecimal bytes that you wish to scan for. Each line in the file represents one virus. The Virus Name for each virus is mandatory, and may be up to 25 characters in length. The double quotes (") are required at the beginning and end of each hexadecimal string.

SCAN will use the string file to search memory, the Partition Table, Boot Sector, System files, all .COM and .EXE files, and Overlay files with the extension .BIN, .OV?, .PGM, .PIF, .PRG, .SYS and .XTP.

Virus strings may contain wild cards. The two wildcard options are:

FIXED POSITION WILDCARD

The question mark "?" may be used to represent a wildcard in a fixed position within the string. For example, the string:

"E9 7C 00 10 ? 37 CB"

would match "E9 7C 00 10 27 37 CB", "E9 7C 00 10 9C 37 CB", or any other similar string, no matter what byte was in the fifth place.

RANGE WILDCARD

The asterisk "*", followed by range number in parentheses "(" and ")" is used to represent a variable number of adjoining random bytes. For example, the string:

"E9 7C *(4) 37 CB"

would match "E9 7C 00 37 CB", "E9 7C 00 11 37 CB", and

would not match since the distance between 7C and 37 is greater than four bytes. You may specify a range of up to 99 bytes. Up to 10 different wildcards of either kind may be used in one virus string.

COMMENTS

A pound sign "#" at the begining of a line will denote that it is a comment. Use this for adding notes to the external virus data file. For example:

```
#New .COM virus found in file FRITZ.EXE from
#Schneiderland on 01-22-91
"53 48 45 45 50" Fritz-1 [F-1]
```

Could be used to store a description of the virus, name of the original infected file, where and when it was received, and so forth.

APPENDIX B: Miscellaneous Application Notes

CHECKING MEMORY FOR VIRUS ONLY

VIRUSCAN can perform a quick check of for viruses in memory only. In this mode, the SCAN program will not check the disk for computer viruses. This option is useful for network administrators who need to check workstations for viruses before allowing them to log on to a LAN but can not run the VSHIELD program due to memory constraints. The command to enter is:

```
SCAN NUL /M /CHKHI
```

By designating NUL as the drive to be scanned, the SCAN program will check system memory for viruses (up to 1088Kb if the /CHKHI option is used) and then return to DOS without scanning any disks. SCAN will set the DOS ERRORLEVEL as it normally does.

VIRUSCAN VALIDATION CODES

If you have installed any new software or programs on your system, and are running VIRUSCAN or VSHIELD with the check validation codes /CV option, you will need to reinstall validation codes to the new files with the add validation codes /AV option of VIRUSCAN. Additionally, the SCANVAL.VAL hidden file containing validation codes for the partition table, boot sector, COMMAND.COM, and system files may have to be replaced. The MS-DOS 5.00 SETVER.EXE file contains self-modifying code and can not have a validation code added to it. The quickest way to update the validation codes is to remove all validation codes from the hard disk and then add them back on by running VIRUSCAN with the /RV and then the /AV options, and then removing the validation code from SETVER.EXE by typing "SCAN C:\DOS\SETVER.EXE /RV" and pressing enter.

NOTE: This applies to any new version of DOS, as well as any programs which you install on your system.

DOS 5 AND REFORMATTING INFECTING FLOPPIES

If you are reformatting infected floppy disks under DOS 5.0, be sure to add the /U switch to the FORMAT command. This tells DOS to do an Unconditional format of the disk, and not to save the original (infected) boot sector of the disk. This should be done to prevent the virus from reappearing by unformatting the disk.